US Department of Education
Student Financial Assistance (SFA)
Modernization Partner Program
Security and Privacy Infrastructure
Task Order 18 Monthly Report 7/10/00

Overview

The office of Student Financial Assistance has made a significant investment in the Modernization Blueprint as the foundation of future process and systems improvements. These processes and systems should be implemented in a secure environment and in a manner that protects the personal, private information of students, parents, and borrowers. This task order proposes development of the security and privacy organization and processes necessary to support such a secure and private environment.

Overall Objectives

The objectives of this proposal are (1) to help SFA secure its current environment and (2) to plan its security and privacy strategy for new initiatives. The task order has the following four outcomes:

- SFA capability to perform risk and vulnerability assessments to identify and document security and privacy risks, recommend mitigating controls and assume business unit responsibility for residual risks as part of its ongoing security and privacy strategy
- A security and privacy organization to support the requirements of current and future business initiatives
- Policies & procedures syndicated with SFA business units and systems administrators
- Communication and training plan coordinated with SFA University and the Director of Communications to ensure that key security and privacy messages are communicated to SFA employees and business partners

Monthly Task Activities

During the period of June 10, 2000 through July 10, 2000 the SFA Security and Privacy Champion approved the modernization Security team’s draft version of the Security and Privacy Guide to Policy. This document was released to SFA management for comment, which should be returned by the end of July.

Meetings were held with eight SFA Security Officers and one System Managers in order to review the security and privacy questionnaires that will be used to: a) survey the subject systems' compliance with GAO / OMB requirements for privacy and security, and to create a database to use to resolve previously reported weaknesses; b) explain the approach for risk assessments of the systems that will support their certification and accreditation process; and c) collect information that will be used later to complete major application security plans targeted for completion Oct 1, 2000. All attendees now have had an opportunity to get clarification where required, and understand better the level of detail required to accomplish the risk assessments.

In the previous month the security team reviewed existing risk assessment reports and created a table of attributes for use in a tracking database. This month a database was created using the commercial off-the-shelf product, Microsoft Access, which is easily customizable by SFA personnel.

The risk assessment team maintains a project plan that shows the risk assessments to be completed by August 18, 2000. This schedule was thought to be at risk of delay due to system manager schedule conflicts. This issue concerning a potential delay was brought to the attention of the Modernization Partner and SFA management. Intervention by the SFA Security and Privacy Champion helped to resolve the concern, which would have led to a four week schedule delay. There continues to be no risk to project cost, but a two-week schedule delay continues to be possible, and will be closely managed.

The security team developed a communication plan outline, and a draft was shared with Mr. Boots who provided comments on June 30, 2000. His comments are being incorporated and work is currently underway to complete this task. This will be the basis for a framework of security program thinking and outline the tasks that are necessary to achieve the vision of an improved security and privacy program entity-wide at SFA.

Major Task Activities Planned Through July 10, 2000

- Complete a Communications Plan;
- Complete Security/Privacy Guidance, based on feedback from CIO review; circulate to security and system contacts in the Channels for review and buy-in;
- Participate in monthly Departmental and security related meetings;
- Begin A-130 security reviews (LO/LC, Pell/RFMS, VDC, and school visits);
- Begin to develop a training program for SFA security personnel;
- Develop requirements for an incident/corrective action tracking system;
- Discuss with acquisitions personnel how to incorporate security features and clearance penalties into performance-based contracts; and
- Begin planning for a SFA Security Awareness Day.

Major Task Activities Completed Through July 10, 2000

- Draft Communications Plan completed June 30, 2000.
- Completed Security and Privacy Policy Guide Draft which is now circulating to security and system contacts in the Channels for review and buy-in;
- Participated in monthly Departmental and security related meetings;
- Began A-130 security reviews of major applications;
- Began to review training courses for SFA security personnel including a review of commercial off-the-shelf materials pertaining to information security and privacy;

- Developed requirements for an incident/corrective action tracking system and created a Microsoft Access database for SFA to use to track resolution; and
- Began planning for an SFA Security training program including Security Officer training and SFA employee security awareness.

Major Task Activities Planned Through August 10, 2000

- Deliver the draft Communications Plan by July 30, 2000;
- Continue A-130 reviews of SFA major applications;
- Modify the draft SFA Security and Privacy Policy Guide;
- Complete the Communications Plan draft;
- Complete the Security and Privacy Organization Plan draft; and
- Participate in monthly Departmental and security related meetings.